Digitally Signed Malware Targeting Gaming Companies

threatvector.cylance.com/en_us/home/digitally-signed-malware-targeting-gaming-companies.html

The BlackBerry Cylance Threat Research Team

The Cylance SPEAR™ team has been working diligently to identify and track relationships between malware using stolen Authenticode code-signing certificates and common command and control (C2) infrastructure. The PassCV group continues to be one of the most successful and active threat groups that leverage a wide array of stolen Authenticode-signing certificates.

Snorre Fagerland of Blue Coat Systems first coined the term PassCV in a blog post. His post provides a good introduction to the group and covers some of the older infrastructure, stolen code-signing certificate reuse, and other connections associated with the PassCV malware. There are several clues alluding to the possibility that multiple groups may be utilizing the same stolen signing certificates, but at this time SPEAR believes the current attacks are more likely being perpetrated by a single group employing multiple publicly available Remote Administration Tools (RATs).

The PassCV group has been operating with continued success and has already started to expand their malware repertoire into different off-the-shelf RATs and custom code. SPEAR identified eighteen previously undisclosed stolen Authenticode certificates. These certificates were originally issued to companies and individuals scattered across China, Taiwan, Korea, Europe, the United States and Russia.

In this post we expand the usage of the term 'PassCV' to encompass the malware mentioned in the Blue Coat Systems report, as well as the APT group behind the larger C2 infrastructure and stolen Authenticode certificates. We'd like to share some of our findings as they pertain to the stolen certificates, command and control infrastructure, and some of the newer custom RATs they've begun development on.

PassCV Background

The PassCV group typically utilized publicly available RATs in addition to some custom code, which ultimately provided backdoor functionality to affected systems via phony resumes and curriculum vitae (CVs). PassCV continues to maintain a heavy reliance on obfuscated and signed versions of older

RATs like ZxShell and Ghost RAT, which have remained a favorite of the wider Chinese criminal community since their initial public release.

SPEAR identified recent PassCV samples which implemented another commercial off-the-shelf (COTS) RAT called Netwire. This tool offers the attacker full control of the victim/host and is perhaps best known for its cross-platform compatibility, which includes support for Windows, Linux, OSX, and Solaris.

Overall, the antivirus (AV) industry has barely kept pace with the PassCV group, and although some samples and families are well detected, the majority of the signed samples continue to have extremely low detection rates.

SPEAR was able to identify several other distinct malware families that we believe to be related to the PassCV group based upon common stolen Authenticode certificates. The Kitkiot and Sabresac (also known as Saber or Excalibur based upon strings in the binaries) malware families were deployed by the group for distinct purposes.

Saber is a custom RAT that periodically queries a web-based C2 server for commands. The only active instances SPEAR was able to identify were hosted on the Chinese code development site 'csdn(dot)net'. Kitkiot variants are commonly installed alongside other types of malware and often included additional functionality, including:

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) capabilities
- The ability to hijack and steal in-game account information and items from multiple online gaming platforms
- In some rare cases these were used for click-through advertising fraud.

The Saber Family

The Saber malware utilizes a custom base64 alphabet for decoding messages from its C2 servers. The malware will decode an obfuscated string found on the site it has been programmed to contact. It will then communicate to the actual C2 for further instructions to execute. SPEAR only observed samples that employed clear-text communication between the victim and the actual C2. The malware accepts any windows shell command the attackers pass back via the C2.

To start the C2 process, Saber samples commonly used blogs on the Chinese-based information technology and development website ‘blog.csdn[dot]net’. The malware executes an HTTP GET request to one or more blog page(s). The malware then looks for the string format 'saberstart. <encoded_string>.saberend' in the response data once the link is retrieved. The data stored between the strings 'saberstart.' and '.saberend' is encoded with a custom Base64 alphabet which contains a follow-on C2 address and a port separated with an uppercase 'W'.

SPEAR developed the following Python snippet to aid in decoding the Saber C2 messages:


Fig1-PassCV-FIXED.jpg

Figure 1: Python Script to Decode Saber C2 Messages

The exact URLs varied among samples, but SPEAR was able to identify the following C2 URLs:

URL: http://blog.csdn[dot]net/u013761036/article/details/45542243
Contained: saberstart.1QXO3Q1s3pfN3Qbu1/fN5pb/ahES+mEMaMSLcgSTjNIPch0PIz.saberend
Accessed: 814,896 times = Number of page visits at the time of writing
Decodes to: gotofindsocketsvcW118.123.19.9W25965#

URL: http://blog.csdn[dot]net//saber00001//article//details//50444103
Contained: saberstart.1QXO3Q1s3pfN3Qbu1/fN5pb/ahIN+mIOcgSR+mIMbo4MbhnSala.saberend
Accessed: 2,167,985 times = Number of page visits at the time of writing
Decodes to: gotofindsocketsvcW123.249.7.226W25982#

URL: http://blog.csdn[dot]net//saber00002//article//details//50444149
Contained: saberstart.1QXO3Q1s3pfN3Qbu1/fN5pb/ahIN+mIOcgSR+mIMbo4MbhnSala.saberend
Accessed: 1,257,722 times = Number of page visits at the time of writing
Decodes to: gotofindsocketsvcW123.249.7.226W25982#

URL: http://blog.csdn[dot]net//saber00003//article//details//50444185
Contained: saberstart.IQ5y5GXp2kTn4QXm2QjO4R1mjNEMaMSMbDnxcDExamAMjNIPch8PIz.saberend
Accessed: 474,514 times = Number of page visits at the time of writing
Decodes to: #gotofindsocketsvcW123.249.81.202W25985#

URL: http://blog.csdn[dot]net//saber00004//article//details//50444188
Contained: saberstart.IQ5y5GXp2kTn4QXm2QjO4R1mjNEMaMSMbDnxcDExamAMjNIPch8PIz.saberend
Accessed: 486,925 times = Number of page visits at the time of writing
Decodes to: #gotofindsocketsvcW123.249.81.202W25985#

URL: http://blog.csdn[dot]net//asdasdasdasddadasd//article//details//50443203
Contained: saberstart.1QXO3Q1s3pfN3Qbu1/fN5pb/ahES+mEMaMSLcgSTjNIPch0PIz.saberend
Accessed: 3,333,320 times = Number of page visits at the time of writing
Decodes to: gotofindsocketsvcW118.123.19.9W25965#'

URL: http://blog.csdn[dot]net//dasdmkdwovcs//article//details//50925619
Contained: saberstart.1QXO3Q1s3pfN3Qbu1/fN5pb/ahIN+mIOcgSR+mIMbo4MbhnSala.saberend
Accessed: 7,475,132 times = Number of page visits at the time of writing
Decodes to: gotofindsocketsvcW123.249.7.226W25982#

URL: http://blog.csdn[dot]net//u013761036/article/details/45542243
Contained: saberstart.1QXO3Q1s3pfN3Qbu1/fN5pb/ahES+mEMaMSLcgSTjNIPch0PIz.saberend
Accessed: 983,239 times = Number of page visits at the time of writing
Decodes to: gotofindsocketsvcW118.123.19.9W25965#

SPEAR was able to successfully emulate the remote C2 server, and during testing we were able to send and remotely execute any command on the (hypothetical) victim system.

Saber Relationships

While researching the Saber family we found a similar .PDB file path in several samples:

"F:\\Excalibur\\Excalibur\\Excalibur\\bin\\oSaberSvc.pdb"
"D:\\Excalibur\\Excalibur\\Excalibur\\bin\\oSaberSvc.pdb"
"F:\\Excalibur\\Excalibur\\Excalibur\\bin\\Shell.pdb"

The malware author originally employed the username ‘Excalibur_C’ (similar to the .PDB file paths) when creating the C2 page:

‘http://blog.csdn[dot]net/u013761036/article/details/45542243’

This was the earliest post that SPEAR was able to identify that contained the encoded Saber commands, with a post date of 2015-05-06 22:20. The same author made numerous other programming related posts in addition to this page:


Fig3-PassCV.png

Figure 2: Excalibur Blog Posts

Since the time we first started working on this write-up, the Saber author has presumably gained some additional attention and it seems the username and icon on the blog were changed as a result:


Fig4-PassCV.png

Figure 3: *Excalibur's New Username*

SPEAR also identified a newer variant during our investigation and subsequent write-up. The compile timestamp indicated that the sample was compiled on August 3, 2016. The newer variant leveraged two different domains:

‘d26yaxxlnmhaem(dot)cloudfront.net’
‘d1wmnlsnh8rftl(dot)cloudfront.net’

The variant also downloaded additional 7-Zip self-extracting archives that ultimately installed the Saber malware onto the infected system. Several other signed variants have also been distributed from the domain:

‘dhd29up7zcdyt(dot)cloudfront.net’

‘Cloudfront.net’ belongs to Amazon’s content delivery network, Amazon CloudFront. This recent move could indicate the attackers are looking for a more robust means of distribution to continue spreading their malware.

The Kitkiot family

Kitkiot malware has been publicly linked to the ‘dns-syn[dot]com’ domain which has direct ties to the group courtesy of Blue Coat Systems’ research. Kitkiot provides backdoor functionality and is commonly installed alongside other types of malware. It has previously been documented and used to perform DDoS attacks, function as a proxy server and perform click-through advertising fraud. We found numerous instances in which Kitkiot variants were written specifically to target online gaming platforms and modify values stored in databases and other online network communications.

Existing public information about this malware family is available via these links:

https://www.threatcrowd.org/listMalware.php?antivirus=Trojan.Kitkiot
http://www.virusradar.com/en/Win32_Kitkiot.A/description

Stolen Certificates and Relationships to PassCV

SPEAR identified roughly eighteen previously undisclosed stolen Authenticode certificates. Interestingly, not all of the certificates were stolen from game companies. It appeared the group had also started to branch out into signed adware. This may seem odd at first, but most security researchers are somewhat numb to the consistent barrage of so-called legitimately signed adware, so a more advanced backdoor signed with the same certificate could easily be overlooked.

The first new connection SPEAR identified was derived from an email address listed in Blue Coat Systems' original report on PassCV. The email address ‘13581641274(at)163.com’ which was used to register the domain ‘aresgame[dot]info’ was reused in 2015 to register the domains ‘fengzigame[dot]net’ and ‘roboscan[dot]net’. Both domains were designed to look like their legitimate counterparts, ‘fengzigame.com’ and ‘roboscan.com’.

SPEAR found several NetWire variants that communicated to subdomains off of the aforementioned domains, and identified another larger cluster of activity that was specifically targeted at game developers using similar variants. **All of the variants communicated to domains that were**

extremely similar to other popular gaming framework websites, and contained code to harvest stored password information as well as log keystroke data.

The C2 domain ‘cocoss2d[dot]com’ mimicked the original website for the Cocos2d gaming framework, ‘http://cocos2d.org/’, used in popular mobile games such as *Badland*. The C2 domain ‘unitys3d[dot]com’ was designed to impersonate the website of the Unity engine, ‘https://unity3d.com/’, a gaming engine licensed across multiple gaming platforms and more recently in popular mobile games like *Pokémon Go.*

Many of the identified samples also contained a common unique mutex, ‘{332222A-33A3-2222-AAAA-3A22AA333}’, which allowed SPEAR to identify a number of additional compromised certificates.

One of the samples identified through this method was:

95a33b0c5f2408adabbebeba6f4c618ba2b392f9dbcd1d9a9ff9db5a519380d8

This led to the discovery of another sample:

ad2a42e4024a320ce763524e17ef7262add649651e2a277b5fc56a9bdc44e449

It was signed with a certificate belonging to AmazGame, a Beijing-based gaming company. The sample also contacted the domain ‘waw.css2[dot]com’, intended to mimic another domain related to the Cascading Style Sheets 2.0 specification:


Fig9-PassCV.png

Figure 4: Beijing AmazGame Certificate

Issued to: Beijing AmazGame Age Internet Technology Co.
Current Status: *Not time valid*
Valid From: 3/16/2012 1:00 AM 6/16/2015 12:59 AM
Thumbprint: B585EA81A25908F25F39088B1FCC239EBF7088D8
Serial Number: 22 CF 7D A7 B7 6F C5 C4 E7 72 25 CF A1 BD A4 97

This in turn led to the discovery of a similar binary via C2 crossover:

78b588fa57b027cda856a05638b25454c59d1896670701f9a8177b8e0c39596d

It was signed with yet another stolen Authenticode certificate:

Figure 5: Syncopate Authenticode Certificate

Issued to: Syncopate LLC

Current Status: Valid

Valid From: 9/24/2015 1:00 AM to 12/24/2017 12:59 AM
Thumbprint: 59EE1A00910451130BB22E06DEB5DCAF1AFAA282
Serial Number: 7E 12 57 33 28 AD F4 5B 6F 3E C3 41 E6 46 29 3A

Syncopate is a well-known Russian company that is best known as the developer and operator of the 'GameNet' platform. GameNet was first identified as being a likely victim of the Winnti group here, although no associated code-signing certificates were identified at that time. Similarly, in that same blog post 'Zemi Interactive' was also identified as being a likely victim from the same attacks. **The evidence presented above strengthens the claim that the Winnti and PassCV groups are closely related**.

During the course of this investigation, SPEAR also identified that NHN's (Naver Corporation) code-signing certificates were compromised, but it appeared to be related to a substantially different attack set that SPEAR hopes to shed some light on in the near future.

Blue Coat Systems originally identified additional connections based upon domain registrant information with the email addresses 'huise123(at)yahoo.com' and 'rebot(at)126.com'. It is possible that the original stolen code-signing certificates were shared among multiple groups and only more recently deployed by the attackers. However, SPEAR has not found any significant evidence to support this hypothesis.

SPEAR identified another sample:

dff0fee3bef9fa2c9c08a6d2c5772e51c1d29522de19301fb389b310e481713f

It was signed using the Beijing AmazGame certificate. The sample beaconed back to the domain 'task.dns-syn[dot]com'. 'bot[dot]dns-syn[dot]com' was previously documented in Blue Coat Systems' write-up as being registered using the email address 'rebot(at)126.com'. This email address was subsequently linked to the domain 'timewalk[dot]me', which was documented in other RATs associated with the Winnti group.

This particular subdomain served a unique purpose, which was to provide additional tasking and to instruct the malware to target a specific online gaming platform. In the case of this particular sample, the targeted gaming platform was 'http://20012.com/'. After analysis of several other similar signed samples, SPEAR found they were all targeted at various individual online and mobile gaming platforms.

SPEAR was able to identify additional samples that utilized these stolen Authenticode certificates, which created an interesting pivot point and led to the discovery of several additional compromised certificates.

Conclusion

The PassCV group continues to be extremely effective in compromising both small and large game companies and surreptitiously using their code-signing certificates to infect an even larger swath of organizations. **Since the last report, the group has significantly expanded its targets to include victims in the United States, Taiwan, China and Russia.**

SPEAR researchers were surprised to find that a good portion of the old infrastructure exposed by Blue Coat Systems remains active to this day. However, it was also apparent that the attackers paid attention to the news, as they let several of the exposed domains lapse and registered extremely similar domains shortly thereafter. The overall operational security of the group has also improved and more recent domains were registered using private WHOIS services and other previously undisclosed email addresses.

Interestingly, most of the malicious binaries were countersigned, which allowed the expired certificates to continue to be valid long past their expiration date. **SPEAR has time and time again observed that this particular "feature" of Microsoft Authenticode Certificates is easily and readily abused by malicious actors.** Even some recent academic papers pointed out that the binary's Authenticode certificate will continue to be valid if a malicious binary is time stamped (countersigned), validly signed and the certificate is subsequently revoked. SPEAR has not identified any samples related to the PassCV group that would support the author of the paper's conclusion, but samples of this nature would indicate that Authenticode signing is indeed rather broken.

While the motivations of the attackers aren't entirely clear, SPEAR believes that the attackers are most likely profiting financially in some way. This could include subverting the in-game economies of the companies they compromise, reselling the stolen code-signing certificates, offering malware signing services or by creating their own private VPN infrastructure from machines within the compromised organizations.

SPEAR identified one binary in particular that fueled this speculation:

8748c19ec86011a77e313e0ea9dd9d0315eed274288585f3663f57e5b8960bdf

The binary was signed with the stolen code-signing certificate from Beijing 'AmazGame' and was named 'Proxy.exe'. The file communicated with a website 'www.proxy456(dot)com', registered using the email-address 'plus3k(at)gmail.com'. This email address was previously used to register the following C2 domains used by the PassCV group from 2012 to 2014:

'1songjiang[dot]info'
'dns-syn[dot]com'
'0pengl[dot]com'
'0penssl[dot]com'
'2likui[dot]info'
'3wusong[dot]info'

Proxy456 claims based on a rough translation to be "China's first integrated cloud proxy software" and at first glance appears to be a semi-legitimate VPN provider. SPEAR also found anecdotal evidence to suggest that the in-game economies of several popular online Chinese gaming communities were being specifically targeted via unique Kitkiot variants.

Even though the motivations of the attackers aren't entirely obvious, the PassCV group continues to be extremely effective at compromising small gaming companies and SPEAR believes it to be only a matter of time before they set their sights on larger organizations.

APPENDIX:

C2 Domains:
115game[.]com
1songjiang[.]info
3389[.]hk
360[.]0pengl[.]com
360antivirus[.]net
64[.]3389[.]hk
amd-support[.]com
auth[.]ncsoft[.]to
bak[.]timewalk[.]me
baidusecurity[.]net
blog[.]unitys3d[.]com
bot[.]1songjiang[.]info
bot[.]360antivirus[.]org
bot[.]duola123[.]com
bot[.]eggdomain[.]net
bot[.]fbi123[.]com
bot[.]fengzigame[.]net
bot[.]godaddydns[.]net
bot[.]ibmsupport[.]net
bot[.]itunesupdate[.]net
bot[.]jjevil[.]com
by[.]dns-syn[.]com
cloud[.]amd-support[.]com
cloud[.]dellassist[.]com
cloud[.]0pendns[.]org
dark[.]anonshell[.]com
dns[.]0pengl[.]com
dns[.]360antivirus[.]org
dns[.]eggdomain[.]net
dns[.]godaddydns[.]net
dns-syn[.]com
down[.]fengzigame[.]net
eggdomain[.]net
fengzigame[.]net
fk[.]duola123[.]com
free[.]amd-support[.]com
global[.]ncsoft[.]to

godaddydns[.]com
gzw[.]3389[.]hk
help[.]0pengl[.]com
hijack[.]css2[.]com
home[.]ibmsupports[.]com
ios[.]0pengl[.]com
intelrescue[.]com
itunesupdate[.]net
jj[.]aresgame[.]info
jj[.]duola123[.]com
jj[.]fbi123[.]com
kasperskyantivirus[.]net
kp[.]css2[.]com
kuizq[.]ddns[.]info
lin[.]0penssl[.]com
lin[.]0pengl[.]com
linux[.]unitys3d[.]com
linux[.]css2[.]com
linux[.]cocoss2d[.]com
ls[.]0pendns[.]org
m[.]css2[.]com
m[.]unitys3d[.]com
mzx[.]jjevil[.]com
new[.]dns-syn[.]com
news[.]0pengl[.]com
news[.]eggdomain[.]net
nokiadns[.]com
ns1[.]0pendns[.]org
ns1[.]amd-support[.]com
ns1[.]appledai1y[.]com
ns1[.]dellassist[.]com
ns1[.]nokiadns[.]com
ns2[.]0pendns[.]org
ns8[.]0pendns[.]org
ns9[.]amd-support[.]com
ns9[.]nokiadns[.]com
nss[.]aresgame[.]info
qqantivirus[.]com
rk[.]mtrue[.]com
rk[.]mtrue[.]net
roboscan[.]net
root[.]godaddydns[.]net
rus[.]css2[.]com
sale[.]ibmsupport[.]cc
sc[.]0pengl[.]com
sc[.]0penssl[.]com
sc.dellrescue[.]com

sc[.]dns-syn[.]com
ssl[.]0pengl[.]com
ssl[.]0penssl[.]com
support[.]godaddydns[.]cc
support[.]godaddydns[.]net
task[.]dns-syn[.]com
test[.]dellassist[.]com
udp[.]jjevil[.]com
udp[.]timewalk[.]me
up[.]roboscan[.]net
update[.]360antivirus[.]net
update[.]0pengl[.]com
update[.]fengzigame[.]net
update[.]nortonantivir[.]us
update[.]css2[.]com
update[.]qqantivirus[.]com
w[.]cocoss2d[.]com
waw[.]cocoss2d[.]com
waw[.]css2[.]com
waw[.]unitys3d[.]com
wsus[.]kasperskyantivirus[.]net
www[.]eggdns[.]com
www[.]iantivirus[.]us
yang[.]0pendns[.]org
zx[.]3389[.]hk
zx[.]css2[.]com
zx[.]duola123[.]com

Suspect Domains Based Upon Registrant:
360antivirus[.]org
appleitunes[.]net
ati-support[.]com
autozhaopin[.]net
cissylee[.]com
fcc8[.]com
fortinetantivirus[.]com
fulita[.]net
itunesupdate[.]org
itunesupdate[.]us
leshi[.]us
qqsecurity[.]net
www[.]proxy456[.]com - proxy provider
zilanhua[.]org

C2 IP Addresses:
101.55.33.106
101.55.64.183
101.55.64.209

101.55.64.246
101.55.64.248
101.79.124.251
101.79.124.254
103.24.152.18
103.25.9.191
103.25.9.193
103.25.9.194
103.25.9.195
103.25.9.200
103.25.9.202
103.25.9.240
103.25.9.241
103.25.9.242
103.25.9.244
103.28.46.79
103.56.102.9
104.199.139.211
106.10.64.250
113.10.168.162
113.30.123.254
113.30.70.209
113.30.70.216
113.30.70.238
113.30.70.254
113.30.103.103
115.23.172.113
116.31.99.65
118.123.19.9
118.123.229.22
118.130.152.246
119.63.38.210
121.156.56.114
121.54.169.39
122.226.186.28
122.49.105.16
123.1.178.39
123.249.7.226
123.249.81.202
14.29.50.66
150.242.210.149
150.242.210.15
150.242.210.160
150.242.210.161
150.242.210.187
150.242.210.195
175.126.40.21

180.210.43.134
182.161.100.3
182.237.3.60
182.252.230.254
183.60.106.205
183.86.194.10
183.86.194.16
183.86.194.42
183.86.194.92
183.86.211.134
183.86.218.167
183.86.218.169
183.86.218.170
184.168.221.40
184.168.221.64
184.168.221.86
192.225.226.74
192.74.232.8
192.74.237.164
199.15.116.59
199.15.116.61
199.83.51.25
202.153.193.90
210.209.116.62
210.4.223.134
211.39.141.23
211.44.42.53
218.234.76.75
219.135.56.175
222.186.58.117
23.252.164.156
23.252.164.238
27.255.64.94
42.121.131.17
45.114.9.206
45.125.13.227
45.125.13.247
58.64.203.13
61.36.11.112
69.56.214.232
98.126.107.249
98.126.193.223
98.126.91.205

Compromised Certificates and Associated Hashes

337 Technology Limited
Not time valid
Valid From: 5/28/2015
Valid to: 5/28/2016
Thumbprint: 99E30AB0B2DAB911190E7A8FA42D4669BE340574
Serial Number: 11 21 B9 67 F0 92 CB F1 92 34 F4 F1 8F 73 0F 4F 76 7B

4769732228d757ee48547fbb27c74495437381f13924039c75c48993f85b930f
6899f3db419b711739120e09320345815717ae79f8091768b1216a142648e54b

Beijing AmazGame Age Internet Technology Co.
Not time valid
Valid From: 3/16/2012
Valid to: 6/16/2015
Thumbprint: B585EA81A25908F25F39088B1FCC239EBF7088D8
Serial Number: 22 CF 7D A7 B7 6F C5 C4 E7 72 25 CF A1 BD A4 97

27463bcb4301f0fdd95bc10bf67f9049e161a4e51425dac87949387c54c9167f
46ca0e17d56b92f2833d59a337c7817b330565e5b09345a3e45be3087b13a3ba
7a4852a81bd546297efb821398609004036aaf578ba7b1488cf98ffaa276cde1
beb9ecc06e1e753224511a52ab36bf7144d2cbbf0d0fcfdb5962897a4c91d861
da29ff774a0facd58bdfb3a45d12024bda401bba91f87077784b5b79251805c9
73d3ae3798e4357e9a162911530f647dcb5f5e07aadad6c9e88a7237135daa56
ad2a42e4024a320ce763524e17ef7262add649651e2a277b5fc56a9bdc44e449
dff0fee3bef9fa2c9c08a6d2c5772e51c1d29522de19301fb389b310e481713f
95a33b0c5f2408adabbebeba6f4c618ba2b392f9dbcd1d9a9ff9db5a519380d8

Beijing Heng Chi Ming Billion Technology Co. Ltd. (北京智明腾亿科技有限公司)
Status Valid
Valid From: 12/14/2015
Valid to: 12/14/2016
Thumbprint: A58B46E37CEBEB20F7948BD781CC1B07C3CB2914
Serial Number: 11 21 33 3A 0B 1E A5 C3 74 87 BE 5B 03 4C E7 E5 48 C2

02922c5d994e81629d650be2a00507ec5ca221a501fe3827b5ed03b4d9f4fb70
7581d381c073d2b67bf2b21f5878855183f9fddf935557021ee6d813b7dda802

Chencheng Cai
Status Valid
Valid From: 1/18/2016
Valid to: 1/18/2017
Thumbprint: B7EDE811E25D1CC7CD70DDC6FAF71C10E25E1D3E
Serial Number: 33 08 CE D5 C1 97 26 54 1B 19 6F 80 5A C5 0C D0

e61e56b8f2666b9e605127b4fcc7dc23871c1ae25aa0a4ea23b48c9de35d5f55
c93a654e21e61a7ae325447091d0f64de4504d35589f60aeb2502fdc54268d8d
200ba936cd229cce4dc0b45a6ab78a5a3e84c5884d56adcc41c7fa7d5b9c831a

EMG Technology Limited
Not time valid
Valid From: 5/15/2015
Valid to: 6/21/2016
Thumbprint: 2CBA7A6D38646D2A2E13D3F27DEEA26A1FCAD0CB
Serial Number: 11 21 C4 FE 70 E9 86 B0 A0 9C EC A4 60 35 9F 98 E5 EE

9edd5b765a6b4d8c3fb8b3998a7b289bfed23b22db68eb1ae30c5495d0d2677a
ef393ea4f3e9ac177593470d84cd4ae6af496212c2a8a5c489e5d34b7e4e5c78

Flyingbird Technology Limited
Not time valid
Valid From: 5/28/2015
Valid to: 6/27/2016
Thumbprint: C3A5D1F89D899B00BA079BD6C943E1BE74D365F4
Serial Number: 11 21 BE 35 5D 77 92 09 D9 11 5C AB 4F 63 99 17 EB 72

21566f5ff7d46cc9256dae8bc7e4c57f2b9261f95f6ad2ac921558582ea50dfb
557647451b5727f7bb56fbf4f00bf29b103db0022b5dbd9741dbfab4bc1def97

Neoact Co.
Not time valid
Valid From: 6/2/2012
Valid to: 7/3/2013
Thumbprint: 8C0B204BB98942D5B750C2FC2258B152DCB1901F
Serial Number: 2B 6E F1 47 1D FC 04 ED 3C B6 42 AC 56 F1 39 E5

0c7b952c64db7add5b8b50b1199fc7d82e9b6ac07193d9ec30e5b8d353b1f6d2

Neoact Co.
Not time valid
Valid From: 6/27/2013
Valid to: 7/28/2014
Thumbprint: 30413DED868E1F152B19F585EF2AE3667252203D
Serial Number: 27 A4 33 CA 2F E7 67 B6 5E B9 6E 43 04 C9 2E 53

28c7575b2368a9b58d0d1bf22257c4811bd3c212bd606afc7e65904041c29ce1
4672f4ebe2d93d52424a92298740994daf232b07e68c13ac88d80f5c64cbfea0
58c39df99155017592abf60ec5a80a339f233bf1eb5dcf2ecf4a5b336cc56e58
aded00e1dab93e15161dc14206d75eccfb4657c360e7e13b6101e00ef26e3399

NHN USA Inc.
Revoked
Valid From: 1:00 AM 11/3/2009
Valid to: 12:59 AM 10/29/2011
Thumbprint: 775141B89F48B71DADC19F13011A46E537E7029C
Serial Number: 2B 5A 38 31 57 EF C7 CD 26 17 EF 32 F0 A7 AC B9

92479c7503393fc4b8dd7c5cd1d3479a182abca3cda21943279c68a8eef9c64b

Polk City Network Technology (Shanghai) Co. Ltd. (北京智明腾亿科技有限公司)
Status Valid
Valid From: 2/4/2015
Valid to: 4/5/2017
Thumbprint: D7D281D4ED737638911CD961E76A7CDD7BFF08B4
Serial Number: 7A 00 AC B7 70 08 A7 21 10 11 0E 0D 66 35 B9 7F

475d1c2d36b2cf28b28b202ada78168e7482a98b42ff980bbb2f65c6483db5b4

Polypower Technology Co.
Status Valid
Valid From: 5/28/2015
Valid to: 6/27/2016
Thumbprint: 01ED0A76185E76575F8FCA667DA73AD290656E03
Serial Number: 11 21 A3 9E 97 47 48 62 3C A6 E3 E4 9A 8B AE B3 ED 3A

24a9bfbff81615a42e42755711c8d04f359f3bf815fb338022edca860ff1908a
8585342d297b4726900e8818817b14042e1a3da5a1497380572a64dcf6d4819c
8944a4ac31b32402ec5c88c4b5645d87f749d3af37c362738f465a9f8e152058

Redduck Inc.
Not time valid
Valid From: 9/24/2013
Valid to: 9/25/2015
Thumbprint: AB879A0A6AF95247415092A5B7FA66B2944E12B9
Serial Number: 0F 66 84 2B 4F 9C 45 8B 72 13 6F 0A E9 69 24 B7

009645c628e719fad2e280ef60bbd8e49bf057196ac09b3f70065f1ad2df9b78
18e6c5968bbe7414278b4fd59ad9a4f1bf9a8a9956dde65f219e9810594381e0
3810d95692613bb4f719d6af64230f9bd6ca7db3a004e089af92a07bed560c01
52de57d6ea3174cf2463f5d32abc7c61d0f0d461c3d543e968a5c09ec0740ddc
67cc48e342d6435792aae1b0576d5707ba4823e32d9ad51fc2ddb5655669b9cd
7dc48bb29c2c9da5a6f60e304714cb2a9b93c735cc3a92522d9fd25799c9a6fa
8736b2d7a73643f0763c74c9fbf50c0109adcabdc794f4973927e3cba4eca220
96377dbd06a57e63e8b3c6b18c92beb2b2e87c9aa155ec11bc7f24ec1e5d7699
b95f611c73c0176e5e8121b0300f4076c147b72115c6706c425a122ff10c10a4
f9778c4e07642f5658285e64297c076877633a4bff9528827d0d3c2108259f72
fb6e4912fca91d99a9747ad2c68ee82da60f787984fadf77aaab40dac7bed3eb
1253e1778714a41b79662dbf9a353afd01a8e72097b3202cc207dd9896c6d7a6
529adca3e873d5db03dc3c8c1ab184ed19135fbe0c8fde80429b7b0072ef41ad

Runewaker Entertainment
Not time valid
Valid From: 11/18/2011
Valid to: 11/18/2014
Thumbprint: 28F5F016604E99C77A444E796F501209F050FC32
Serial Number: 59 76 83 B6 8E F6 B0 C8 BE 2D 85 A2 12 B5 19 10

03aafc5f468a84f7dd7d7d38f91ff17ef1ca044e5f5e8bbdfe589f5509b46ae5
1ade09a1c54800787dc63d09b76f69fd2cca8b4bbb63c8c39c720628ea37471a
1e8fe3ee0fffc8144c6252035c7f247bac129e7aa5c4537cf5e3f25531e04a67
28123038d24ef74a396a2a88700f947bfa72cdddd6bc56524c113a529a3423cd
2936ae7f7099c32e701c3b956a7eb7ef800bf5748122c883819c834ec61af44a
2d0be850cc137540d163e9c035f4c99f27caa5bb8cdb1cea6182b5da49cff0f2
5a723f65da58bdcfc639f557f490213ca8c5009db0ddde7fffef8d2bcf3966f5
5d6986f440e89f4a309a62f9df8ea5989a8880229dc02b132dd1bb3d0e0083d1
774efc29c19254714c986423aee968bfb03daf4ce79fddbef4ec3b4b5eee3f8f
7eecb8af098ead93e9bf2d5a4e86ff3f172e94566d296f061971410036a22a0f
830d48b2c6de780783e697346a6afe96c6e33654d85b71bb86627b88f09f298c
916a2b4d9c6a5f4fd5333f4d165cb8ad1479253d8141b6087ed412f3a1b059c2
9941fd97327d54a18209d0bb1f36992a18a3809aa8d163e7fe80193a4348610a
a65ca7dbfdb15d88ba6d37a521e5dda768388ed9d48184859d71be3afb57de16
ab65eebe0f96d3787893329992670ff97621c76e2d8c1be366c00429c944350b
d6f3151ed4fb00b766cf70df678b932c616a122c6c9f2a62e33d4a103465f8af
df013d3b048931a23dcc9db63e6b7d76dfc4373a3f41a274744179b6546e4cd1
fb1ab5a92af54263f1dd6bdf5657ac0c4b52d9639acecb4b339a82c5650b9a6f
e7a721682ff2b00c00da50a51c87e9bc7cb93292e4cf42bb04185c3392fdec41

Syncopate LLC
Status Valid
Valid From: 9/24/2015
Valid to 12/24/2017
Thumbprint: 59EE1A00910451130BB22E06DEB5DCAF1AFAA282
Serial Number: 7E 12 57 33 28 AD F4 5B 6F 3E C3 41 E6 46 29 3A

0cf6d9a5aa3b390f97f20b2fbd2cd9df76c5bb018c997c26d2e16eb44127c624
2d752e8a6e42d4b1d14e4400cccb5f1bda3dccd1264d09f4bb2fefb6b6f5048a
48f8c31530d621de0cb401fb32c282eecc91bdac602aac9bd4ddbe8c6a6ceb39
78b588fa57b027cda856a05638b25454c59d1896670701f9a8177b8e0c39596d
9375e3482163cbe388a49317dce8eb7bb23761a29a06ae9a9c4f11628f60d1f3
b941aaf32e4102fad862bf8c4b36d5f0932a4388dd3b7502f68233cb6a9a8ae9

Taiwan Shui Mu Chih Ching Technology Limited
Not time valid
Valid From: 3/6/2015
Valid to: 3/4/2016
Thumbprint: D76AC870EBD12FBBE587D48E1640E76EA499B86E
Serial Number: 11 21 27 47 4D E0 10 DA 49 D3 1D 0E E8 19 3E AC 2D 0E

4f4fa26bc26fd90c64dd3b347a92817b67b64506c025248330aa69b00b97051f

Woodtale Technology Inc
Not time valid
Valid From: 7/11/2012

Valid to: 7/16/2015
Thumbprint: EF00842D40EAC4FDFC2BF62E00829AD83C6046AE
Serial Number: 04 53 F5 E1 43 79 37

7c32885c258a6d5be37ebe83643f00165da3ebf96347150390978154020 4752e

Wuxi Kai Yang Electronic Technology Co. Ltd. (无锡凯扬电子科技有限公司)
Status Valid
Valid From: 11/20/2015
Valid to: 11/20/2016
Thumbprint: D0EF4A086EDE76B39863104F8832706950CBB053
Serial Number: 57 BE 1A 00 D2 E5 9B DB D1 95 24 AA A1 7E D9 3B

016250b7d62e49ba386404cc6db38cb65323d26cf80bc94e2810d5ab9e59fff2
2acc78ece9cb1a7865341e69fb72097a2debf2c82f41976554132bf6d3181c25
ea63f6a26a18fbeae7c9e042a43988f938503126b485238e3d44f75ae30868bc

Yang Liu
Status Valid
Valid From: 6/20/2016
Valid to: 11/26/2016
Thumbprint: B467B21C4CA4EA7E3AE55FF03D4540900AACC97E
Serial Number: 2F 04 6D 17 50 F5 F5 27 BD 6F 57 50 3A 7C AA 07

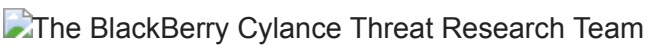
Zemi Interactive Co.
Not time valid
Valid From: 7/9/2013
Valid to: 8/9/2014
Thumbprint: 6F889C3FE070D493A79B698D1FC7D7E428D18F90
Serial Number: 45 05 E9 AC 8D 28 8D 76 3A 10 88 ED 1E 2C 8A 60

14da1add073c48c57da5d14ab55c461bca2ece5d06d5a3d563f14eda56d806fa
16c4e5c26e072d3b50b58d3c2b1e3985405a686867dedc75d75bd44d84ac4434
24e3ea78835748c9995e0d0c64f4f6bd3a0ca1b495b61a601703eb19b8c27f95
320b73e5cee7590a529001af9cea5f36520adc5c50ef48c72912e2dae7283ac6
3f50ced416c9d7feaa0ad6fb16be1f1289590b497024e20c34b139c2b5194e7c
5f851ffcee7f301bfcffc3c023a78611f6a1264575ffbafa1f3bc420b27f7eac
66a1514ea0b833d9108f7ad1ec39a568cedcb46839f956ab330fb72791fd827d
77a15c0e45c1dfa42d135321576c725c40f890d95e9ad44bdabeae9eb5d71a9f
81986d0559db51317ca03f1d4102f8ddf86451ec18ba9649129c7704373cfed1
86e091ebce3ee9e9de15bc600bed01ddaa6668794d40d70bbef02386304fd7c4
b42bb2221490b763a84714140d75c8eb3189caac0f5940626d07b8303eccedec
b46786252512197a96093ab4cb906a851f75f82da7ad850c220a44002f39c739
b84d90acd1a43e560c7e3ae12922cceb286a30dd3e1cc02089f1359a7286a671
cbd62862584f8544aadca0b4f8f3405576378f5542b776bc4e91f384ad146440
ec49983235a079c72c32212f0e216fb8ebd2354b6936c39cfd736c4a2dd018e4
4e6b30db935e41231a108cba1c5d4cacde03cf262e9e85d24387950ae5a369c6

Zemi Interactive Co.
Status Valid
Valid From: 8/25/2015
Valid to: 9/24/2016
Thumbprint: 3E508596F683E30FE1A86504B3B35A44A513A141
Serial Number: 76 31 1C 06 EB 80 09 5E B5 20 D0 2B DE 7F AC 1F

0f290612b26349a551a148304a0bd3b0d0651e9563425d7c362f30bd492d8665

NOTE: This is an ongoing investigation by the SPEAR Team. The full report will be made available on Cylance.com in the near future.



About The BlackBerry Cylance Threat Research Team

The BlackBerry Cylance Threat Research team examines malware and suspected malware to better identify its abilities, function and attack vectors. Threat Research is on the frontline of information security and often deeply examines malicious software, which puts us in a unique position to discuss never-seen-before threats.